EXPEDITED PROCEDURE UNDER 37 CFR § 1.116
GROUP ART UNIT 2137; EXAMINER Z. Davis

PATENT

IBM Docket No. **POU920000179US1** **09/740,457**

REMARKS/ARGUMENTS

At present, the examiner has maintained the objection to applicants' specification which, as far as applicants' attorney can discern, is a minor typographical error which has been corrected above. Additionally, applicants' Claims 1 and 2 stand rejected under 35 USC § 102(b) based upon the article by Tenca et al. Claim 3 stands rejected under 35 USC § 102(a) based upon the cited article by Compaq titled "Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment." Claims 4 through 6 stand rejected under 35 USC § 103(a) based upon the combination of the Compaq article and the article by Tenca et al. In light of the remarks presented below, all three of these rejections are respectfully traversed. Accordingly, Claims 1 through 6 remain pending in the present application.

As a matter of formality, it is noted that the minor spelling error on page 3 of applicants' specification has been corrected herein. Other informalities have been corrected in earlier amendments. Accordingly, it is respectfully request that the examiner withdraw the objection to applicants' specification.

Attention is now directed to the three art based rejections of applicants' claims. The rejection of applicants' Claims 1 and 2 under 35 USC § 102(b) based on Tenca et al. is considered first.

It is first noted that the examiner's characterization of applicants' Claims 1 and 2 as employing a calculating engine that is based upon the Montgomery multiplication algorithm is correct. However, applicants use this engine in ways that are not taught nor suggested by the art cited. In particular, it is noted that applicants' Claims 1 and 2

are not directed to methods or devices for carrying out Montgomery multiplication. Instead, it is noted that both of these claims are directed to methods and apparatus for producing the value *A* mod *N*. Furthermore, it is noted that applicants' process and apparatus both operate by partitioning the input variable *A* into blocks of *k* bits each. This is one of several significant differences between applicants' claimed invention and the teachings found in Tenca et al.

Before considering the specific teachings of Tenca et al, it is instructive to consider the specific steps that are referred to in applicants' Claim 1. In particular applicants' Claim 1 recites a digital processing method for determining *A* mod *N* using what is essentially a Montgomery multiplication engine. In particular, it is recited that this particular engine is capable of processing words that are *k* bits long. In other words, applicants' have recited a process which is capable of employing a smaller sized Montgomery multiplier to carry out the determination of *A* mod *N* when *A* is in fact of a size larger than that which could ordinarily be processed by such an engine.

Furthermore, in applicants' method, as recited in Claim 1, there is a three-step process. In the first step, this smaller engine is operated with two inputs as specified. In particular, it is noted that one of these inputs is the low order bits A_0 in the representation of *A* as $A_1 2^{mk} + A_0$. Next, applicants add the result produced by operating this engine to the value A_1 to produce a second result. Again, in applicants' step 3, the same, smaller Montgomery multiplying engine is operated with inputs being outputs from the adder and the value 2^{+2mk} mod *N*. This process produces the desired value *A* mod *N*. It is the applicants' position that none of these specific steps is recited or suggested by Tenca et al.

EXPEDITED PROCEDURE UNDER 37 CFR § 1.116
GROUP ART UNIT 2137; EXAMINER Z. Davis

Attention is now specifically directed to what can reasonably be assumed to be the teachings from the cited article by Tenca et al. It is first noted that Tenca et al. is directed to Montgomery multiplication. Furthermore, and most significantly herein, Tenca et al. is directed to a scalable architecture for Montgomery multiplication. In order to achieve this scalable architecture, Tenca et al. require that one of the input variables to the multiplier be represented and processed bit by bit. In this regard, the examiner's attention is directed to Page 97 of the Tenca et al. article where they indicate that words are marked with superscripts and that bits are marked with subscripts. In particular, the multiplier X in the process is described as an m bit vector $X = (x_{m-1}, \ldots x_1, x_0)$. In absolutely every instance where methods for computation are recited for carrying out Montgomery multiplication, the multiplicand X employed bit by bit. Accordingly, it is seen that anyone of ordinary skill in the art following the teachings found in Tenca et al. would not only be led to but would be required to employ algorithms in which one of the operands is processed bit by bit and not in any larger chunks. In this regard, the examiner's attention is further directed to the coded algorithm set forth on pages 97 and 98 of the Tenca et al. article wherein it is seen that, in every place where the multiplier X is employed, the individual bits are used in the calculation, not chunks or larger pieces of data are employed. In this regard, the examiner's attention is also specifically directed to Figures 6, 7 and 8 where, in each instance, bit values are employed for the operand X.

Accordingly, those of ordinary skill in the art following the teaching of Tenca et al., when employing a Montgomery multiplier, would be required for scalability to provide one of the operands as a bit string with all operations being carried out sequentially using single bit data values from the X multiplier operand.

Accordingly, it is seen that even if Tenca et al. is read as disclosing a method of determining *A* mod *N* using a Montgomery multiplication algorithm (which it is not), the specific algorithm and method recited in applicants' Claim 1 and Claim 2 are nowhere taught or suggested by Tenca et al. As applicants have previously pointed out, Tenca et al. teach that at least one operand input to the Montgomery multiplying operation is processed bit by bit. In contrast, it is seen that the calculating engine which is described in applicants' specification processes bits *k* at a time. In particular, the examiner's attention is directed to applicants' Figure 4 in which the portion of such a processing element is shown.

To the extent that Tenca et al. teach the utilization of a Montgomery multiplication process for calculating *A* mod *N*, the examiner's attention is directed to the center portion of page 96 of the subject article. Therein, there is described a two-step process for producing the result *a* mod *N* (in Tenca et al. their lower case "*a*" corresponds to applicants' "*A*" and their "*M*" corresponds to applicants' "*N*"), and it appears that they disclose a two-step process using the Montgomery method for multiplication in which the first step is to produce the M-residue $\bar{a}$. This step requires two inputs *a* and r^2. In a second step, the inputs to Montgomery multiplier are $\bar{a}$ and 1. In both of these processes, the input to the Montgomery multiplier is the entire value of the variable "*a*" from which the value *a* mod *M* is to be computed. There is no teaching, disclosure or suggestion in the cited article that the input parameters are larger than that which is capable of being processed by the Montgomery multiplier. In particular, there is no teaching, disclosure or suggestion that the input parameter "*a*" is partitioned in any way whatsoever. In point of fact as describe above, the only way in which Tenca et al. employ a Montgomery multiplier is through individual bit operations, not with chunk operations. In point of fact, Tenca et al. require this aspect for their scalability criteria.

EXPEDITED PROCEDURE UNDER 37 CFR § 1.116
GROUP ART UNIT 2137; EXAMINER Z. Davis
PATENT
***IBM Docket No.* POU920000179US1 09/740,457**

It is pointed out that a rejection under 35 USC § 102 is a narrow ground of rejection. It requires each and every recited claim element to be described in a single cited document. None of the recited steps in applicants' Claim 1 are taught, disclosed or suggested by the Tenca et al. article. In particular, it is specifically noted that applicants' Claim 1 is directed to a digital processing method employing a calculating engine which processes words of *k* bits each to produce the result *A* mod *N* where *A* is a variable having many more bits than *k*. Furthermore, the input variable supplied to the calculating engine recited in applicants' Claim 1 is, in each instance, different from any input variable employed in the Montgomery multiplier seen in the article by Tenca et al.

While the discussion above has primarily focused upon applicants' Claim 1, as noted by the examiner, applicants' Claim 2 is sufficiently similar to have been covered by the same arguments as described above.

Accordingly, it is seen since there are significant differences between applicants' Claims 1 and 2 and that which is described in the article by Tenca et al., it is seen that the rejection of these claims cannot be sustained under 35 USC § 102. It is therefore respectfully requested that the rejection of these claims be withdrawn.

In light of the incorporation of the recitations of Claim 4 into Claim 3, it now appears that the rejection of Claim 3 under 35 USC § 102(a) based upon the article by Compaq is now rendered moot. Accordingly, the comments provided below are also now seen to be applicable.

EXPEDITED PROCEDURE UNDER 37 CFR § 1.116
GROUP ART UNIT 2137; EXAMINER Z. Davis

Attention is next directed to the rejection of applicants' Claims 4 through 6 under 35 USC § 103(a) based upon the combination of the teaching found in the documents by Compaq and Tenca et al. In this regard, it is noted that all recited claims refer to the utilization of a calculating engine which accepts as inputs variable of *k* bits. It is further noted that, as described above, the methods and devices described in applicants' Claims 4 through 6 all produce ultimate outputs having sizes much greater than *k* bits. Nothing in the art cited by the examiner teaches, discloses or suggest such a process or apparatus. Furthermore, as discussed above, the teachings of Tenca et al., specifically require that any algorithm employed utilizes the value of one of the variables in a bit by bit fashion. This is clearly not the teaching of applicants. In particular, in all of the cited claims, applicants' calculating engine accepts two inputs *x* and *y* each of which is *k* bits long. As pointed out above, Tenca et al. specifically teach against such a process. In point of fact to provide the scalability of Tenca et al., bit by bit processing for one of the operands is an essential feature. Those of ordinary skill in the art who are following the teachings of these two documents would not be led to provide a doubly *k* bit partitioned method such as that recited in applicants' Claims 4 through 6. In point of fact, it is noted that applicants' Claim 4 through 6 all recite a process in which a *k* bit calculating engine is employed which operates on smaller chunks of data but yet still produces results that apply to much larger groups of data. In this regard, it is noted that applicants' claims specifically indicate that the calculating engine operates on words that are *k* bits long but that the modulo N result is *mk* bits long and that *m* is the smallest integer for which $mk \geq n + 2$, where *n* is the number of bits in *N*.

Accordingly, it is seen that applicants' process produces results that are applicable to outputs having a size of *mk* bits while the engine itself operates on words that are only k bits in length. This is nowhere taught, disclosed or suggested in any of the art cited by the examiner. Accordingly, those of ordinary skill in the art having the

two cited documents before them would not in any way be led to a structure such as that claimed in applicants' Claims 4 through 6. It is therefore respectfully requested that the rejection of applicants' Claims 4 through 6 under 35 USC § 103 be withdrawn.

It is noted that the response does not require the payment of any additional fees. It is further noted that the present response is being submitted within the two-month time interval as set forth in 37 CFR § 1.136. It is therefore requested that the examiner provide the applicants with an advisory action no later than April 19, 2005. If an advisory action is not to be forthcoming by that time, applicants also request that the examiner telephonically advise applicants of this fact so that applicants may respond appropriately within the time period provided for appeals.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless applicants have argued herein that such amendment was made to distinguish over a particular cited document or combination of documents.

Accordingly, it is now seen that all of the applicants' claims are in condition for allowance. Therefore, early notification of the allowability of applicants' claims is earnestly solicited. Furthermore, if there are any matters which the Examiner feels could be expeditiously considered and which would forward the prosecution of the instant application, applicants' attorney wishes to indicate his willingness to engage in

EXPEDITED PROCEDURE UNDER 37 CFR § 1.116
GROUP ART UNIT 2137; EXAMINER Z. Davis

any telephonic communication in furtherance of this objective. Accordingly, applicants' attorney may be reached for this purpose at the numbers provided below.

Respectfully Submitted,

MAR. 17, 2005
Date

Lawrence D. Cutter
LAWRENCE D. CUTTER, Sr. Attorney
Reg. No. 28,501

IBM Corporation, IP Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

Phone: (845) 433-1172
FAX: (845) 432-9786
EMAIL: cutter@us.ibm.com